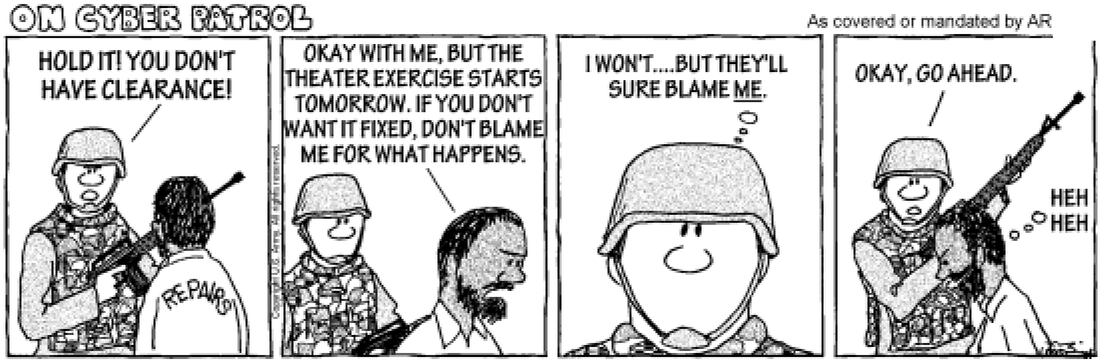
Mind Games at the Cyber Perimeter

February 2006


ON CYBER PATROL
As covered or mandated by AR
HOLD IT! YOU DON'T HAVE CLEARANCE!
REPAIRS
OKAY WITH ME, BUT THE THEATER EXERCISE STARTS TOMORROW. IF YOU DON'T WANT IT FIXED, DON'T BLAME ME FOR WHAT HAPPENS.
I WON'T....BUT THEY'LL SURE BLAME ME.
OKAY, GO AHEAD.
HEH HEH

Ever since you were a kid people have tried to get information out of you using many different techniques. Here a few examples I'm sure you've heard before.

Forceful: Tell me or I'll hit you so hard your dog will die!

Subtle: Of course if you don't let me in, Mom might find out about that broken glass.

Emotional: That's OK Billy. Why should a mother know about her son's life, what with my high blood pressure and all?

Threatening: OK Soldier, don't give me password access to your computer. But if the Major finds out you're not in compliance you'll be pulling guard duty outside of Mosul for the rest of your life.

The technique used in this month's On Cyber Patrol cartoon is common and surprisingly effective. When faced with the threat of being blamed for something or facing the anger of a superior many people, both military and civilian will break or bend rules, to avoid blame or perceived punishment. It's often a quick decision based on an emotional reaction to staying out of trouble. What the person trying to gain access is counting on is that the victim will not take the time to think down the road to the potential damage and loss that could result from allowing a breach of security.

It's all about gaining access to information or ways of obtaining information. Even though it seems easy to spot, too many people -- both military and civilian -- give others access to proprietary information because of simple yet effective social engineering techniques. Trying the technique depicted in the graphic is just the tip of the iceberg. Other techniques include using official looking or sounding emails or other communications to obtain secure information. This technique called phishing is just another way enemy forces and common criminals use our fears of doing something wrong or not following instructions against us.

Using social engineering is an important element in our daily lives. It is part of the convincing process. It is part of raising children. What it should not do is break down a soldier's duty to protect critical Army resources, information and lives.

Never allow unauthorized access to any computer or communication equipment. No matter what you are told, the threat to you and your fellow soldiers for allowing unauthorized access far outweighs risk of what is perceived to be the consequence of not divulging that information. Ensure that all personnel allowed access fully meet the clearly defined access protocols as stated in AR 25-2. Don't allow would be saboteurs to convince you that you will be held responsible for negative results if you refuse them access.

This isn't a matter of memorizing regulations. It is a matter of common sense. If you have responsibility to secure something, secure it. It's the same as standing guard at a perimeter. Even the most innocent-seeming breach of that security can result in significant damage, disruption and potential loss of life.